CyberVigilance™

A PROTEUS TECHNOLOGIES CYBER SOLUTION

#ACTB4URHACKD

RESEARCH REMEDIATE RESPOND

"Not everybody agrees on what's funny, obviously" - Tim Meadows

The newest discovered ransomware called **CryptoJoker** proves to be anything but amusing and although it doesn't appear to have been widely distributed as of yet, it is an entirely functional ransomware that could see increased distribution in 2016.

No Laughing Matter

CryptoJoker uses AES-256 encryption that demands a ransom to recover your files. As soon as it encrypts your data, CryptoJoker scans the drives on your computer, including mapped network drives, for files with certain extensions. When it finds targeted extensions, it will encrypt the file and change the filename so it has a '.crjoker' extension appended to it.

While CryptoJoker is encrypting your data, it also sends your information to Command & Control servers located across the Internet. This information includes the date, username, and hostname. CryptoJoker will also remove Shadow Volume Copies and disable Windows automatic startup repair to make it impossible to recover any files.

At this time there is no known method to decrypt files encrypted by CryptoJoker for free.

Act Before You're Hacked

If you are unsure how to protect your network or file shares from CryptoJoker or other security threats, contact PROTEUS at CV@proteuseng.com to find out how our CyberVigilance™ services can keep YOUR files safe against these types of malware.

PROTEUS TECHNOLOGIES Outsmart.